TESTIMONY OF DAVID M. STONE
ASSISTANT SECRETARY OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION
DEPARTMENT OF HOMELAND SECURITY

ON 9/11 COMMISSION RECOMMENDATIONS ON CIVIL AVIATION SECURITY

BEFORE THE
SUBCOMMITTEE ON AVIATION
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
UNITED STATES HOUSE OF REPRESENTATIVES

AUGUST 25, 2004

Good morning Mr. Chairman, Congressman DeFazio, and Members of the Committee. Thank you for this first opportunity to appear before the Subcommittee as the confirmed Assistant Secretary for Transportation Security to discuss the recommendations of the National Commission on Terrorist Attacks Upon the United States to improve civil aviation security. This Subcommittee has consistently played a prominent role in enhancing aviation security and has vigorously carried out its oversight responsibilities. I look forward to working in partnership with you in the months ahead to continue to strengthen aviation security in accordance with the recommendations of the Commission and through other important initiatives.

The Commission's Report is a powerful, potent reminder to each of us at the Transportation Security Administration (TSA) of the significance of our security mission. Turning the pages of the Report and reflecting upon the Commission's findings about the events of that tragic day, TSA employees across the country and in Washington reaffirm their commitment to carrying out their duties with diligence, thoroughness, and professionalism. I commend the Commission for the painstaking work and probing analysis that went into this huge endeavor. I am focusing carefully on each of the Commission's recommendations for transportation security and incorporating them into TSA's efforts to counter the continued threats of terrorism in civil aviation and in the other modes of transportation.

As the Commission recognized, "[t]he U.S. transportation system is vast and, in an open society, impossible to secure completely against terrorist attacks." However, we are confident that we can significantly protect against threats to the security of our transportation system—yet protect privacy and civil liberties—by continuing to evaluate vulnerabilities throughout the transportation system, prioritize the risks and focus resources accordingly, and implement layers of security across all modes of transportation. TSA, the Border and Transportation Security Directorate (BTS), and the Department of Homeland Security (DHS) as a whole, the Department of Transportation (DOT), and transportation stakeholders have been working collaboratively to provide

seamless transportation security. Ensuring that our Nation's transportation systems are secure must be accomplished through effective partnering among Federal, State, local, and private industry entities.

I agree with the Commission that no single security measure is foolproof, and, accordingly, we must have multiple layers of security in place to defeat the more plausible and dangerous forms of attack against transportation. Since the creation and stand up of TSA nearly three years ago, and with the establishment of BTS and DHS, we have advocated layered security and designed our aviation security programs around the concept of a "system of systems." We continue this approach as we focus our attention on security in other modes of transportation as well.

Working together with the Information Analysis and Infrastructure Protection (IAIP) directorate and BTS, TSA continually assesses the threats, risks, vulnerabilities, and consequences of potential attacks on transportation systems using a threat-based risk-management approach. Effective, strategic, threat-based planning results from evaluations of available intelligence and assessments of criticality, vulnerability, and recoverability information. These allow us to form a picture of the overall risk environment and devise effective strategies to mitigate identified vulnerabilities. Collectively, DHS is meeting the responsibility for coordinating these efforts in the transportation sector with all DHS components and DOT modal administrations.

Currently, all threat information received by DHS is carefully analyzed for its potential impact on any U.S. critical infrastructure or system at home or overseas. The IAIP directorate receives information regarding threats to the homeland from DHS entities and the U.S. Intelligence Community, as well as from our State, territorial, tribal, local, and private sector partners. If we conclude that warnings to industry and field operators or operational adjustments are warranted, our response can take a variety of forms. Top government decision makers are alerted immediately, as well as industry stakeholders. IAIP and/or TSA disseminate specific warnings, advisory information, or countermeasures, where appropriate, to local law enforcement and the transportation industry.

As part of our ongoing threat analysis, each morning I chair a comprehensive review with TSA leaders of the intelligence assembled in all sectors of transportation and the threats that may be implied by this intelligence. We review and discuss in detail daily reports from Federal Security Directors (FSDs) around the country on incidents in aviation security. We also hold a weekly intermodal stakeholder teleconference to share unclassified intelligence as well as to provide information on TSA security programs and to solicit input. This weekly teleconference has proven to be a very effective communication tool.

I would like to focus on some of the key recommendations of the Commission concerning civil aviation, highlight actions TSA is taking in line with the recommendations, and discuss our plans for addressing the recommendations in the future.

Risk-Based Decision Making

The Commission recommended that "[t]he U.S. government should identify and evaluate the transportation assets that need to be protected, set risk-based priorities for defending them, select the most practical and cost-effective ways of doing so, and then develop a plan, budget, and funding to implement the effort. The plan should assign roles and missions to the relevant authorities (Federal, State, regional, and local) and to private stakeholders."

Homeland Security Presidential Directive 7 (HSPD-7) directed the establishment of "a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks." HSPD-7 assigned responsibility to DHS to develop a National Plan for Critical Infrastructure and Key Resources Protection (National Plan) that will establish roles and responsibilities of Federal, State, local and private entities for each sector's protection, including the civil aviation sector. The Secretary has assigned responsibility for drafting the National Plan to IAIP, and TSA has been asked to coordinate development of the Transportation Sector Specific Plan (SSP).

TSA is working in close coordination with DHS components, with DOT and its modal administrations, including the Federal Aviation Administration (FAA), with other key Federal, State, local, and tribal agencies, and with appropriate private sector stakeholders in developing this plan. The Transportation SSP will delineate roles and responsibilities between the stakeholders and will provide a "roadmap" for identifying critical infrastructure and key resources, assessing vulnerabilities, prioritizing assets, and implementing protection measures. The Transportation SSP will help ensure that these efforts are systematic, complete, and consistent with the efforts in the other sectors.

DHS, through TSA and other related agencies, will build on the foundation of the Transportation SSP to provide overall operational planning guidance on transportation security. Furthermore, as part of the Transportation SSP, TSA will work with DOT modal administrations, including the FAA, and DHS components to develop modal security plans and ensure that they are integrated into an effective concept of operations for management of the transportation sector's security. Development of the National Plan, and of the Transportation and other SSPs, is well underway, and DHS anticipates completion before the end of the year.

As the HSPD-7 mandated National Plan and its supporting SSPs are implemented, DHS will complete a comprehensive prioritized list of critical assets and vulnerabilities that will address all sectors, including the Transportation Sector. This is one of the primary tools that DHS will use to allocate limited resources in a risk-based and cost-effective way, as recommended by the Commission.

Secure Identification

The Commission recommended that the Federal government set standards for the issuance of sources of identification, noting that at many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure people are who they say they are and to check whether they are terrorists.

I know that this Subcommittee has consistently expressed an interest in the potential of biometric technologies to provide for secure identity verification. Research in biometric technologies continues to be integral to several TSA initiatives, including the Registered Traveler (RT) pilot program, the Transportation Workers Identification Credential (TWIC) program, infrastructure access control programs, and employee screening. TSA coordinates with US-VISIT and U.S. Customs and Border Protection (CBP) to leverage research and initiatives already underway. Establishing standards for sources of identification is a complex process involving efforts to ensure access identification does not reinforce an assumed identity, measures to reduce false matches, appropriate levels of performance for biometric technologies, safeguards for identity information, and other functionality. The research and testing now underway through existing programs are critical steps toward establishing effective standards for secure identity verification.

TSA's RT pilot program is designed to improve the security screening process by helping TSA align screeners and resources with potential risks. Registered travelers will be positively identified at the airport through biometric technology. Passengers who have volunteered for this program will go through expedited security screening at specially designated lanes. Approved registered travelers will be directed to a designated checkpoint lane where they will provide their biometrics (fingerprint and iris scan) and, in some locations, a Registered Traveler Smart Card containing biometric information for identity confirmation. Registered travelers and their carry-on bags will still go through primary screening, but more extensive secondary screening will be largely eliminated, unless they alarm the Walk Thru Metal Detector. We expect this program to provide frequent travelers with a high level of security and an expedited screening experience. Passengers and airlines report that they are very pleased with the RT pilots now underway. The RT program is being piloted at Minneapolis-St. Paul International Airport, Los Angeles International Airport, George Bush Intercontinental Airport (Houston), Boston Logan International Airport, and Ronald Reagan Washington National Airport.

TSA's TWIC program is testing alternatives for developing and potentially implementing a secure credential that could be used to mitigate possible threats posed by workers in transportation industries with fraudulent identification. The TWIC program is intended to enhance security controls applicable to the variety of transportation personnel whose duties require unescorted access to secure areas. TSA recently began the prototype phase in developing the TWIC. In the prototype phase, the TWIC program uses biometrics to verify identity and prevent duplicate enrollments. TWIC will verify identities by comparing the cardholder's finger(s) with the fingerprint template stored securely on the card's integrated circuit chip. The TWIC prototype and supporting measures will test how best to assess the risks of transportation workers entering secure areas of our

national transportation system, with nearly 150,000 workers from aviation, maritime, rail, and ground modes of transportation expected to participate at over forty sites in six states. The President's FY 2005 request includes spending authority to begin implementing the TWIC concept within parameters that will be defined by the Administration after completion of the prototype assessment, which is expected to last seven months.

Biometric studies are an important component in TSA's 20-Airport Access Control Pilot Program, to test operationally and evaluate access control technologies. These pilots will include use of fingerprint and iris scan biometric technologies to validate the identification of employees accessing an airport restricted area. Additional technologies will be incorporated into these pilots such as Radio Frequency Identification (RFID) to control vehicle access, intelligent video analysis to differentiate between persons who are authorized and not authorized to be in specific areas, portable card readers and fingerprint recognition technology at a vehicle gate, and vehicle gates that are activated by an iris biometric recognition system. Overall, TSA has initiated 10 access control pilot programs, and data gathering will continue through the end of calendar year 2004. Information obtained during these projects will be shared with other Federal agencies, as well as industry representatives to provide them with information about specific technology capabilities as they design systems to protect their facilities.

In addition to exploring technological improvements in access control, TSA is actively strengthening safeguards for access to Security Identification Display Area (SIDA) and sterile areas of our Nation's airports. TSA currently requires fingerprint-based criminal history record checks of all airline and airport workers who have access to SIDA and vendor employees who work in the sterile area of an airport. As part of its "system of systems" strategy to securing SIDA and sterile area access, TSA is in the process of strengthening background checks. TSA has begun conducting enhanced background checks on all commercial aviation workers in the U.S. who have access to the secure and sterile areas of our Nation's airports. These enhanced checks include advanced analysis of the best available information to determine whether an individual poses a potential terrorist threat and will focus on preventing known terrorists from gaining credentials allowing access to SIDA and sterile areas.

Knowing of the Subcommittee's continuing interest in screening of airport workers, I would like to report that airport sterile area workers are now required to go through physical screening at TSA security checkpoints. On July 6, 2004, TSA issued new Security Directives (SDs) that strengthen these standards by requiring enhanced background checks and improved access control for airport employees working in restricted areas.

Improved Use of Watchlists

The Commission recommended that improved use of "no fly" and "automatic selectee" lists should not be delayed while the planning for a successor to CAPPS continues. The Commission also said that this screening function should be performed by TSA and it should utilize the larger set of watchlists maintained by the Federal government. We

agree, and we are pleased to report that a significant amount of progress since 9/11 that is fully consistent with this recommendation.

Prior to 9/11, there were fewer than 100 names on the "no-fly" list. Today, TSA provides carriers with "no-fly" and "selectee" lists that have been dramatically expanded. New names are being added every day as intelligence and law enforcement agencies submit new names for consideration. This places a significant burden on air carriers, reservation systems, and airline passengers, and we appreciate their efforts and patience as these lists continue to expand. In addition, we have reduced the number of passengers whose names are erroneously matched to the "no-fly" list. Continued expansion will be possible as integration and consolidation of various watchlists by the Terrorist Screening Center (TSC) progress and as the U.S. Government is able to assume the responsibility for conducting the list comparisons.

TSA is an active participant in international activities designed to promote effective collaboration in the effort to restrict terrorist movement. TSA routinely shares intelligence with the United Kingdom and Canada and foreign air carriers who provide service to the U.S. In partnership with the Department of State, TSA leads U.S. efforts to strengthen aviation security at the global level by promoting the adoption of best practices within international organizations that set the pace and standards for aviation security. TSA works with the Department of State to support the implementation of existing standards and adoption of new, stronger standards via international organizations, such as the Group of Eight (G-8), the International Civil Aviation Organization (ICAO), and the European Union. TSA and State actively pursue the alignment of U.S. and foreign aviation security requirements through bilateral agreements and security representation at U.S. embassies and consulates.

TSA is performing security checks on international flight crew on domestic and international passenger and cargo flights bound for the U.S. In December, 2003, TSA received new information about specific threats to aviation security related to crewmembers on flights to, from, and overflying the U.S. and issued a series of Security Directives (SDs) and Emergency Amendments (EAs) significantly expanding the scope of crew vetting.

On the issue of CAPPS II, DHS is nearing completion of a significant review of a next-generation passenger prescreening program that meets our goals of using the expanded no-fly and selectee lists to keep known or suspected terrorists off of planes, moving passengers through airport security screening more quickly, and reducing the number of individuals unnecessarily selected for secondary screening, all the while fully protecting passengers' privacy and civil liberties. A revised program will incorporate the valuable lessons we have learned from existing passenger prescreening programs and improve aviation security. It will also likely remove the responsibility from air carriers for conducting watch list comparisons. We look forward to working closely with Congress, the privacy and civil liberties communities, and the aviation community to execute a new passenger prescreening program in the most cost-efficient and least-intrusive manner possible.

Improvement of Screening of Passengers and Property

The Commission recommended that "[t]he TSA and the Congress must give priority attention to improving the ability of screening checkpoints to detect explosives on passengers. As a start, each individual selected for special screening should be screened for explosives. Further, the TSA should conduct a human factors study…to understand problems in screener performance and set attainable objectives for individual screeners and for the checkpoints where screening takes place."

I want to note first that TSA already does conduct screening for explosives at passenger checkpoints according to protocols designed to apply available explosives detection resources in the most effective way currently possible. However, we understand that more comprehensive methods must be found for the long term.

TSA has initiated 4, soon to be 5, pilot projects to test operationally and evaluate explosives detection trace portals for persons. TSA is also about to initiate an additional 4 pilot projects to operationally test and evaluate document scanners that will detect traces of explosives. Both of these efforts will provide TSA with increased capabilities in the detection of explosives that might be secreted on an individual, rather than within a bag. Additionally, TSA, through its R&D program, is preparing to publish a request for proposals for development of automated explosives detection technology for carry-on items to increase explosives detection capabilities overall at the passenger screening checkpoint. We intend to review deployment options in the near future.

Numerous human factors engineering studies have been conducted, ranging from ergonomics and injury prevention to the best way to present an X-ray image to maximize the ability of a screener to identify a threat while an image is on the screen.
In July 2003, TSA completed a comprehensive Passenger Screener Performance Improvement Study, which focused on human factors and utilized the principles of Human Performance Technology (HPT). The study team validated desired screener performance, examined screener practices, and determined factors that influence the gap between these two states. Utilizing the study's findings, in October 2003, BTS and TSA crafted a Short-Term Screening Performance Improvement Plan containing nine broad initiatives and 62 specific action items to provide tangible improvements in screener performance and security. The broad initiatives included use of the Threat Image Projection (TIP) system in X-ray machines to identify specific strengths and weaknesses in X-ray screeners' abilities to recognize and respond to threat objects. TIP is a critical element in our overall plan to continuously improve screener performance. Currently, all of TSA's X-ray machines are TIP-ready and uploaded with a 2,400 simulated threat image library. Other initiatives included improved FSD support and accountability, improvements to the initial and recurrent training programs for screeners and screener supervisors, extensive covert testing conducted by TSA's Office of Internal Affairs and Program Review, improved workforce management utilizing SABRE scheduling software and greater hands-on involvement by FSDs and their staff, revisions to the Screening Checkpoint Standard Operating Procedures, providing high-speed IT

connectivity between airport checkpoints and training computers, and ongoing pursuit of new technologies to identify threats more accurately while decreasing false positives.

We have initiated more extensive human factors engineering studies to identify behavioral and environmental factors that affect screening performance. Working together, staff with expertise in human resources management, recruitment, training, operations, and human factors research assists TSA in developing and refining training requirements and curriculum, as well as operating protocols to enhance performance. Additionally, our human factors team works with our screener workforce to ensure screening equipment deployed and under development is user-friendly for operators. These efforts are also focused on evaluating screener test results and recommending changes to screener duties based on studies monitoring screener performance under various conditions, including stress conditions.

By June 2004, TSA had completed 57 of the 62 specific identified actions. Three action items are still in progress, of which two are expected to be completed this month. A third action item is expected to be completed in the first quarter of Fiscal Year 2005.

As part of the Short-Term Screening Performance Improvement Plan, TSA's Office of Internal Affairs and Program Review (OIAPR) conducted covert testing at 152 airports. Once TSA's screening improvement initiatives had been implemented nationwide, OIAPR retested 44 airports between January and March 2004. Since testing began after deployment of TSA screeners in November 2002 to the present, there has been a 70 percent improvement in covert test results.

TSA also seeks to improve screener performance through monthly town hall meetings at which the screener workforce can communicate concerns and recommendations to senior management and staff, as well as ongoing briefing of screeners on current intelligence about weapons and terrorist subjects as information is received. In addition, TSA is establishing a longer-term plan to improve screener performance. Areas that are being examined include establishment of improved training facilities at airports and reconfiguration of checkpoints.

The Commission also raised a concern regarding the screening and transport of checked bags and cargo, and, specifically, the Commission recommended directing greater attention and resources to reducing or mitigating the threat posed by explosives in vessels' cargo holds, expediting the installation of advanced (in-line) baggage-screening equipment, and requiring every passenger aircraft carrying cargo to deploy at least one hardened container to carry any suspect cargo. The Commission also recommended that efforts be intensified to identify, track, and appropriately screen potentially dangerous cargo in both the aviation and maritime sectors. BTS and other DHS organizations, including the Coast Guard, have been working in a variety of ways to improve the security of cargo, and this is being reviewed in light of the Commission's recommendations.

TSA has made steady progress in improving the number and capability of the explosives detectors in place at our airports and our related procedures. For checked baggage, there are both short-term and long-term research and development efforts underway. TSA's short-term (1-3 years) effort, the Phoenix Project, focuses on three areas: (1) significantly improving currently deployed systems; (2) combining emerging technologies such as quadrupole resonance and x-ray diffraction with currently deployed systems; and (3) taking advantage of evolutionary new systems, technological improvements, and advancements in computed tomography.

Simultaneously, new technologies will be developed under the Manhattan II project, part of the Next Generation EDS Program, announced publicly on April 16, 2004. TSA intends to select multiple proof-of-concept efforts over the course of approximately one year. Upon completion of this phase, TSA will evaluate the results and award system development contract(s) for those concepts and technologies with demonstrated potential.

TSA is working with the vendors of the currently tested and approved blast resistant (hardened) baggage/cargo containers to decrease the weight of each unit and to lower purchase costs to make them a more economical and operational solution. While these efforts continue, TSA has expanded efforts to develop blast resistant aircraft cabin, overhead bin, and cargo liners. TSA has partnered with the FAA and aircraft manufacturers to develop other technologies that could be installed or incorporated into the initial design and manufacturing of aircraft to mitigate the impact of an explosion either in the cabin or in the cargo hold area of the aircraft.

TSA continues to strengthen air cargo security. In November 2003, TSA issued security directives to air carriers requiring random inspection of air cargo transported on both all-cargo and passenger aircraft. In December 2003, Secretary Ridge approved TSA's comprehensive air cargo security Strategic Plan, which will serve as the roadmap for TSA's efforts to improve security in the air cargo shipping arena for the next three to five years. A Notice of Proposed Rulemaking that will put "teeth" in the Strategic Plan is being finalized and contains many significant regulatory enhancements for air cargo related to indirect air carriers, air carriers, and airports. TSA has also hired or has deployed over 250 Aviation Security Inspectors (ASIs), who enforce aviation security regulations generally, plus 100 all-cargo ASIs brought on in FY 2004 to improve air cargo compliance rates. TSA inspectors closely monitor air carrier compliance with these directives, and the carriers are meeting or exceeding the required level of physical inspection.

TSA's air cargo R&D efforts will continue into Fiscal Year 05 to identify the appropriate technology to screen air cargo. In Fiscal Year 2004, TSA's R&D budget for air cargo was set at $55 Million, and for Fiscal Year 2005 the President's budget has designated an additional $55 Million for air cargo R&D. Currently TSA is (1) selecting vendors to develop explosives detection technology for containerized cargo and automated US Mail inspection, (2) initiating six pilot projects to conduct a cargo characterization study to determine the feasibility of using currently certified explosives detection technology (EDS and ETD) to screen cargo while new systems are under development, and (3)

supporting the pulsed fast neutron analysis technology pilot sponsored by CBP and TSA for containerized cargo screening.

Additionally, earlier this year, TSA deployed our Known Shipper Database, which has provided increased vetting and control over air cargo shippers. The program is an information-based approach to cargo security. The Known Shipper program is used by passenger air carriers, Indirect Air Carriers (IACs or freight forwarders), and all-cargo carriers who transfer cargo to passenger planes. Known Shipper previously operated in a decentralized mode, with each carrier and IAC responsible for maintaining its own separate database of known shippers. In an effort to strengthen the program and to reduce its vulnerability to exploitation, TSA has developed and implemented a centralized Known Shipper database that allows all participating carriers to verify the known status of a particular shipper. Shippers in the Known Shipper database are verified against a variety of watch lists and terrorist data, and their status is centrally recorded. Shippers accepted in the program are deemed to pose a lower risk and therefore allowed to transport cargo on passenger aircraft. More than 450,000 known shippers are already included in the database, and the system is currently averaging about 1,000 inquiries a day. Because the database is now centralized and managed by TSA, it can easily be modified to respond to new threats to aviation.

General Aviation Security

The Commission expressed concern that General Aviation (GA) continues to present an aviation security challenge.

I am aware that as vulnerabilities within commercial aviation are reduced, GA may be perceived as a more attractive target and consequently more vulnerable to misuse by terrorists. However, there can be no such thing as "one size fits all," when thinking about security in the GA sector. TSA is committed to making threat-based, risk-managed decisions, balanced with common sense.

TSA is engaged in the launch of the Transportation Risk Assessment and Vulnerability Evaluation tool that will allow GA airports operators to examine their airports and assess vulnerabilities. The tool focuses on the characteristics of the facility and an inventory of its countermeasures. Initially the tool will be made available to approximately 5,600 public use GA facilities across the country. TSA will capture the input from these self-assessments and plot the data on the criticality matrix assessment. A trial set of airports will be used to test the tool prior to its roll out.

TSA has published an Information Publication, "Security Guidelines for General Aviation Airports" containing an "Airport Characteristics Measurement Tool" and made this available to GA airport operators and industry groups. The tool helps operators to self-assess risk and apply TSA-recommended mitigation measures.

Additionally, TSA has conducted many security site visits and vulnerability assessments. Partnering with industry groups and operators, TSA has developed security best practices to mitigate risk at maintenance, repair, overhaul, and storage facilities for larger aircraft.

TSA has issued Security Directives to operators of New York City air tour helicopters and the heliports that support the operations to address current intelligence information and to mitigate the threat of an airborne attack carried out through access to air tour helicopters. TSA worked closely with stakeholder associations representing the helicopter community and local operators to craft measures that would provide the necessary level of security and avoid adverse impacts on operators. The issuance of these directives highlights our ability to immediately act on information received by the agency and to work with those sectors of the aviation community that are not regulated by TSA to provide a threat-based, risk managed, approach to securing our transportation systems.

In collaboration with National Business Aviation Association, TSA developed the Transportation Security Assured Access Program, a set of security procedures that aircraft operators can put into place to increase the security of their operations. In 2003, the Association, in partnership with TSA, initiated a pilot project at Teterboro Airport in New Jersey. Operators who put these procedures into place and were approved by the Association to apply for a certificate from TSA were authorized to operate internationally without a waiver.[1] In 2004, the Association expanded the program to include corporate aircraft operators based at Morristown, New Jersey, and White Plains, New York, on a trial basis.

Before I conclude, I would like to highlight several recent TSA accomplishments in matters that have been of importance to the Subcommittee. First, I am pleased to report that TSA now posts security checkpoint wait times on our Internet website. Historical wait times are provided by airport, day of the week, and time of day to help travelers plan for their next flight. Also, TSA's Aviation Partnership Support Plan has been extremely successful in preventing delays during the high summer travel season at the Nation's airports while maintaining high standards for security. The average wait time was 3.8 minutes and the average peak wait time was only 12.2 minutes from June 1 through August 11th for the top 40 largest airports nationwide. We remain on course to meet the demands of upcoming Labor Day travel peaks as well. Your early expressions of concern about potential delays were instrumental in the formulation of TSA's comprehensive plan and helped to solidify the partnership of air carriers, airport operators, and their associations to see it through successfully.

In addition, you have my assurance that among my first official actions as Assistant Secretary, I am pushing greater decision making authority to the field. Using Boston Logan Airport as a test-bed, we are piloting an approach to recruitment, hiring, and training of screeners that is focused on the FSD, and this approach will be extended to additional airports over the remainder of the summer. Under this new approach, FSDs will have greater flexibility to obtain the right people, at the right time, at the right location. In May, TSA completed instructor training for nearly 700 screener and FSD

[1] General aviation aircraft operators wishing to fly to the U.S. from other countries must stop in one of seven portal countries: Japan, Canada, Mexico, the Bahamas, England, Scotland, Wales, and Northern Ireland. Operators can apply for a waiver if they wish to proceed directly to the U.S. without going through one of these countries. Operators with TSA Access Certificates need not go through one of these portal countries or obtain a waiver to enter the U.S.

staff personnel to empower them to conduct both new hire and cross training at the airport level. In June, each FSD became responsible for determining the level of training support required to meet the specific needs of the airport. These changes will help TSA to be more responsive to the needs of individual airports while maintaining high standards for aviation security.

I want to assure the Subcommittee of my cooperation and determination in working to carry out the Commission's important recommendations. As Assistant Secretary of TSA, I am guided by several key principles. The first is leadership—leading people, leading the development and deployment of technology to use our resources efficiently and effectively, and leading change. The second principle is partnership. I have worked to develop and promote a spirit of partnership with all of our stakeholders that are involved in protecting, operating, and using our transportations systems. Last, and just as critical, is the principle of friendship. It is vital to the success of TSA that we inspire the trust and confidence of the American people and their elected representatives in the Congress.

This concludes my prepared remarks. I will be happy to answer any specific questions Subcommittee members may have.